REMARKS

The Office examined claims 1-7 and rejected same. With this paper, various of claims 1-7 are amended, none are canceled, and new claims 8-11 are added, so that claims 1-11 are now pending.

Changes to the existing claims not prompted by the Office action

With this paper the claims are amended by replacing "characterized" with "comprising." Applicant respectfully submits that this amendment does not affect the scope of the claims. See MPEP § 2111.03 (the transitional term "comprising" is synonymous with "characterized by"). The claims now consistently use "comprising" to introduce limitations on which applicant relies for patentable weight. Also, the phraseology "step" or "steps" is eliminated from the method claims to help prevent the method claims from being erroneously interpreted as reciting "step plus function" elements.

In addition, the main claims (1 and 6) are changed in a way believed to be mere clarification, and claim 4 is changed in a way believed useful in more distinctly claiming the invention.

Also, as noted below, new claims 8-11 are added.

Objections to Specification and Drawings

Specification and drawings are objected to because of informalities. With this paper, relevant paragraphs of the specification are amended and replacement drawing of figure 1 is provided. Support is at page 6, lines 31-32.

Rejections under 35 USC §112

Claims 5 and 7 are rejected under 35 USC §112, second paragraph, as being indefinite. With this paper, claims 5 and 7 are amended to make more clear that these are claims to a computer program product and a system, respectively, and are recited as including limitations of method claim 1 and apparatus claim 6, respectively, for economy in prosecution. It is believed that with the changes made to these claims, the bases for the rejections have been obviated. Withdrawal of the rejections is respectfully requested.

Rejections under 35 USC §103

The Office rejected claims 1-7 on the following grounds:

At page 4 of the Office Action, claims 1-3 and 5-7 are rejected under 35 USC §103(a) as being unpatentable over Sarvar Patel, "Analysis of EAP-SIM Session Key Agreement" (Patel hereinafter) in view of Dharmapurika et al., "Longest Prefix Matching Using Bloom Filter" (Dharmapurika hereinafter).

At page 7 of the Office Action, claim 4 is rejected under 35 USC §103(a) as being unpatentable over Patel in view of Dharmapurika and further in view of US Pat. App. Publication 2005/002209 (hereinafter Aguilera).

With regard to claims 1 and 6, the present invention provides a solution to various GSM EAP/SIM authentication problems, and in particular, provides a method for determining whether a candidate RAND[1] included in a RAND challenge (in an EAP/SIM authentication message exchange) is *not* one of one or more previously used RANDs. Claim 1 is to a method, and claim 6 to a corresponding apparatus, i.e. to an apparatus able to operate according to the same method. Claim 1 recites a method including a step of encoding the (one or more) previously used RANDs using a data structure consisting of an ordered set of components all having a starting value of zero, but the value for a component may be set to one based on the previously used RANDs. The data structure is then checked to determine whether the candidate RAND is *not* one of the previously used RANDs. Importantly, all of the bits of each previously used RAND are used in determining whether to set the value of a component to one. More specifically, each component has a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set of components, the component is pointed to by any of a plurality of pointer values (i.e. the pointer value is a number that indicates the position of the component in the ordered set) each based on *all the bits* of a respective one of the previously used RANDs. Figure 2 is helpful to an understanding of this encoding.

---

[1] A RAND, as illustrated in the application, is e.g. a 128-bit random number used with a root key K_i (up to 128 bits) to generate a 64-bit key K_c and a 32-bit value SRES included in a RAND challenge.

One embodiment of the data structure is based on a so-called Bloom filter. Claim 2 encompasses such an embodiment. From Wikipedia:

> The Bloom filter, conceived by Burton H. Bloom in 1970, is a space-efficient probabilistic data structure that is used to test whether or not an element is a member of a set. False positives are possible, but false negatives are not. Elements can be added to the set, but not removed (though this can be addressed with a counting filter). The more elements that are added to the set, the larger the probability of false positives.

The Office concedes that the primary reference Petal does not disclose the recited (claims 1 and 6) encoding of previously used RANDs to provide a data structure and the recited checking of the data structure to determine whether a candidate RAND is not one of the previously used RANDs. For such disclosure, the Office relies on Dharmapurika, which provides an algorithm for IP routing lookup based on Bloom filter theory. The Office thus asserts that it would have been obvious at the time of the invention, for one of skill in the art to modify the teachings of Petal according to the teachings of Dharmapurika, so as to arrive at the invention.

In fact, though, Petal *teaches away* from the invention. At section 2.2.1, Petal teaches that:

> There is actually *no solution to this problem* [of providing for session independence] as long as one is working with GSM triplets as the fundamental source of keying. The above solutions to strengthen the 64 bit [*sic*] to 128 bits are of no use in creating session independence, and it's hard to see how one could do it easily.
>
> One approach possible but *not practical* is for the client *to store all the past RAND vectors* its [*sic*] seen and to make rue that they are not repeated. ...
>
> Since its [*sic*] not practical to store all past values, perhaps the client can *store the most recent n RAND values* and make sure they are not repeated. This may *give some practical protection* in practice. Actually the whole RAND vector doesn't need to be stored, *just a part of the RAND*, for example 32 bits *can be stored* and looked for repeats [*sic*]; ... .

So the most that can be learned from Petal is that one should store only part of the most recent n RAND values, and then look for repeats. *In direct contrast*, the invention requires determining a data structure of components each having a starting value of zero, but the value is set to one if, based on the order of the component in the ordered set of components, the component is pointed to by any of a plurality of pointer values (i.e. the pointer value is a number that indicates the position of the component in the ordered set) each based on *all the bits* of a respective one of

previously used RANDs. On the contrary, the best Petal could suggest is that *only some of the bits* be used in looking for repeats (because of memory limitations).

Now per the MPEP at 2143.01 (VI), a proposed modification cannot change the principle of operation of a reference:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Applicant therefore respectfully submits that altering the teachings of Petal according to the teachings of Dharmapurika (and so arriving at the use of a Bloom filter), is not obvious.

Further, although Dharmapurika provides a general description of Bloom filter theory and an algorithm for *IP routing lookup* based on Bloom filter theory, *Dharmapurika does not suggest using a Bloom filter in a RAND challenge.* Thus, Dharmapurika does not teach or suggest either the encoding or the checking steps recited in claim 1, so that even the combination fails to teach or suggest these steps. In other words, the teachings of Dharmapurika are limited to applications of Bloom filter theory to IP routing lookup. Further, Dharmapurika is only interested in finding a match,[2] not determining that there is *not* a match, as required by claims 1 and 6. Thus, there is no suggestion in either Dharmapurika or Petal of applying Bloom filter theory to guarding against repeats in a RAND challenge. Applicant therefore respectfully submits that the invention as in

---

[2] At page 201, right-hand column, Dharmapurika explains that the problem being solved is "to search variable-length address prefixes in order to find the longest matching prefix of an I destination address [for each packet traversing a router] and retrieve the corresponding forwarding information."

claims 1 and 6 is thus patentable over the combination of Petal and Dharmapurika, because per the MPEP at 2143.03:

> To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

For these reasons, at least claims 1 and 6 are believed patentable over the applied art.

Further with regard to claim 3, though, Dharmapurika nowhere teaches or suggests using a RAND to set to one the value of one or another component of a data structure of ordered components. For the Office to assert this, applicant respectfully submits that Dharmapurika would at least have to teach or suggest using a destination IP address as a hash function value in constructing a Bloom filter. But Dharmapurika does not teach or suggest this. Further, it is not clear that a destination IP address *could* be used as a hash function value, since unlike a RAND or a hash of a RAND, an IP address is not random (because some addresses are more likely to occur than others).

Further with regard to claim 4, the Office asserts that Dharmapurika teaches a data structure that is a multi-part data structure with each part having an upper limit on the number of RAND values it can indicate as one of the previously used RAND values, relying on page 211, Figure 10b, showing "Bloom filters of length m/2." With this paper, claim 4 is changed to more distinctly claim the invention in respect to the multi-part data structure embodiments encompassed by claim 4, by further requiring that each (of two) parts has values based on only some of the previously used RANDs, and wherein all most recently received RANDs received are used in determining component values in only one of the parts, and further wherein when an upper limit is reached for the one of the parts, another of the parts is reset. Applicant respectfully submits that none of the applied references teach or suggest this further limitation, for which support is provided beginning at page 11, line 5, through page 12, line 2.

New claims

New apparatus claims 8 recites limitations corresponding to apparatus claim 6. New claims 9-11 correspond to method claims 2-4, which therefore provide support. The new claims are believed distinguished over the applied art for the same reasons as claims 6 and 2-4.

Conclusion

For all the foregoing reasons it is believed that all of the claims of the application are in condition for allowance and their passage to issue is earnestly solicited. The undersigned Applicant's agent urges the Examiner to call to discuss the present response if anything in the present response is unclear or unpersuasive.

Respectfully submitted,

Date: 16 July 2007

James A. Retter
Agent for the Applicant
Registration No. 41,266

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468-0224
Tel.: (203) 261-1234
Cust. No.: 004955